

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of

Inventors: Yoshikazu ISHII
Application No.: New PCT National Stage Application
Filed: March 10, 2005
For: WIRELESS LAN ACCESS AUTHENTICATION SYSTEM

CLAIM FOR PRIORITY

Assistant Commissioner of Patents
Washington, D.C. 20231

Dear Sir:

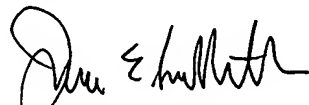
The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested for the above-identified application and the priority provided in 35 USC 119 is hereby claimed:

Japanese Appln. No. 2003-137830, filed May 15, 2003.

The International Bureau received the priority document within the time limit, as evidenced by the attached copy of the PCT/IB/304.

It is requested that the file of this application be marked to indicate that the requirements of 35 USC 119 have been fulfilled and that the Patent and Trademark Office kindly acknowledge receipt of this document.

Respectfully submitted,



James E. Ledbetter
Registration No. 28,732

Date: March 10, 2005

JEL/spp

Attorney Docket No. L9289.05107
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L STREET, NW, Suite 850
P.O. Box 34387
WASHINGTON, DC 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200

PCT/JP03/12125

24.09.03

日 本 国 特 許 庁

JAPAN PATENT OFFICE

Rec'd PCT/PTO 10 MAR 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2003年 5月15日

出 願 番 号
Application Number: 特願2003-137830
[ST. 10/C]: [JP2003-137830]

REC'D 13 NOV 2003

WIPO

PCT

出 願 人
Applicant(s): 松下電器産業株式会社

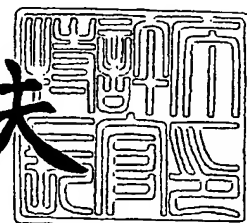
**PRIORITY
DOCUMENT**

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2003年10月31日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 2900750359

【提出日】 平成15年 5月15日

【あて先】 特許庁長官殿

【国際特許分類】 H04Q 7/20

【発明者】

【住所又は居所】 神奈川県横浜市港北区綱島東四丁目3番1号 パナソニックモバイルコミュニケーションズ株式会社内

【氏名】 石井 義一

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100105050

【弁理士】

【氏名又は名称】 鷺田 公一

【手数料の表示】

【予納台帳番号】 041243

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9700376

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 無線LANアクセス認証システム

【特許請求の範囲】

【請求項1】 無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、

前記複数の無線LANネットワークの各ゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置とアクセスされた無線端末装置のアクセス認証を行いアクセス認証された無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を配布する認証サーバとを有する前記複数の無線LANネットワークを統合して管理するセンター局と、を備え、

前記各無線LANネットワークは、各無線LANネットワーク内の無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に該無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理手段と、前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した無線端末装置が前記アクセス管理手段により前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理手段と、を具備することを特徴とする無線LANアクセス認証システム。

【請求項2】 前記ゲートウェイ装置は、前記アクセス管理手段及び前記暗号鍵管理手段を有することを特徴とする請求項1記載の無線LANアクセス認証システム。

【請求項3】 前記アクセス管理手段は、前記各無線端末装置のアクセス時間又は通信パケット量の少なくとも一方のアクセス量を管理し、前記アクセス量が所定量に達した時点で前記無線端末装置に再認証を要求する管理部を有することを特徴とする請求項1又は請求項2記載の無線LANアクセス認証システム。

【請求項4】 前記無線端末装置はID情報が記録されているSIMカード

又はUIMカードを備えており、前記無線端末装置のアクセス認証時の認証用IDとして前記SIMカード又はUIMカードに記録されているID情報を用いることを特徴とする請求項1から請求項3のいずれかに記載の無線LANアクセス認証システム。

【請求項5】 無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、前記複数の無線LANネットワークの各ゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置とアクセスされた無線端末装置のアクセス認証を行いアクセス認証された無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を配布する認証サーバとを有する前記複数の無線LANネットワークを統合して管理するセンター局と、を備えた無線LANアクセス認証システムにおいて前記無線端末装置のアクセス認証を行う無線LANアクセス認証方法であって、

前記各無線LANネットワークが、各無線LANネットワーク内の無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に該無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理ステップと、前記アクセス管理ステップで前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理ステップと、を有することを特徴とする無線LANアクセス認証方法。

【請求項6】 無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、前記複数の無線LANネットワークの各ゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置を有する前記複数の無線LANネットワークを統合して管理するセンター局と、を備えた無線

LANアクセス認証システムにおいて前記無線端末装置のアクセス認証を行う認証サーバであって、

前記認証サーバは、前記センター局に配置され、前記各無線LANネットワークの所定のアクセスポイント部に前記無線端末装置がアクセスするときのアクセス認証を行うアクセス認証手段と、前記各無線LANネットワークの各ゲートウェイ装置に対して前記無線端末装置がアクセスする無線区間の暗号鍵を一括して配布する暗号鍵配布手段と、を有することを特徴とする認証サーバ。

【請求項7】 無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、前記複数の無線LANネットワークの各ゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置とアクセスされた無線端末装置のアクセス認証を行いアクセス認証された無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を配布する認証サーバとを有する前記複数の無線LANネットワークを統合して管理するセンター局とを備えた無線LANアクセス認証システムにおける前記各無線LANネットワークのゲートウェイ装置であって、

前記ゲートウェイ装置は、前記センター局のセンター局ゲートウェイ装置とのデータ信号及び制御信号の送受信を行う送受信手段と、前記各無線LANネットワーク内の無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際にこの無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理手段と、前記アクセス管理手段により前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理手段と、を有することを特徴とするゲートウェイ装置。

【請求項8】 前記ゲートウェイ装置のアクセス管理手段は、前記各無線端

末装置のアクセス時間又は通信パケット量の少なくとも一方のアクセス量を管理し、前記アクセス量が所定量に達した時点で前記無線端末装置に再認証を要求する管理部を有することを特徴とする請求項7記載のゲートウェイ装置。

【請求項9】 無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、前記複数の無線LANネットワークの各ゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置とアクセスされた無線端末装置のアクセス認証を行いアクセス認証された無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を配布する認証サーバとを有する前記複数の無線LANネットワークを統合して管理するセンター局とを備えた無線LANアクセス認証システムにおいて使用される無線端末装置であって、

前記無線端末装置は、前記センター局の認証サーバによりアクセス認証される際に用いるID情報が記録されたSIMカード又はUIMカードを有することを特徴とする無線端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部を有する複数の無線LANネットワークが統合されたネットワークにおける無線端末装置の無線LANアクセス認証システムに関する。

【0002】

【従来の技術】

近年のオフィス及び企業内などのローカルエリアネットワーク、及び公衆ネットワークにおいては、IEEE802.11bなどの無線LAN規格を利用した無線LANネットワークが運用されている。このような無線LANネットワークでは、ESSIDやMACアドレスによる認証、及びWEP(Wired Equivalent Protocol)による無線区間の暗号化が行われている。しかしながら、このような認証及び暗号化は、セキュリティの脆弱性が指摘さ

れている。このため、最近では、IEEE 802.1Xプロトコルを用いたRADIUS (Remote Authentication Dial-In User Service) サーバによるアクセス認証、及びWEPキーの動的な配布をサポートする機器による無線区間の暗号化を行うネットワークが構築されるようになってきている。

【0003】

一方、このようなネットワークの普及に伴って、ユーザのより快適な通信を実現するために、各ネットワーク内及び各ネットワーク間での無線端末装置のハンドオーバーの高速化が必要となってきた。

【0004】

従来、このようなハンドオーバーの高速化を実現する通信方式として、ユーザの無線端末装置がハンドオーバーする可能性のあるアクセスポイント部において事前に認証済み状態を作り、ハンドオーバー時の前記アクセスポイント部に対する認証を不要として速やかな通信を行うようにした方式が提案されている（例えば、非特許文献1参照）。

【0005】

この従来の通信方式では、次のような動作が実行される。

【0006】

(1) ユーザのログイン時、前記ユーザの無線端末装置と認証サーバ間とで通常の認証を行う。

【0007】

(2) 前記ユーザがログインしたアクセスポイント部と前記認証サーバとは、この後前記ユーザが通信で用いる認証ヘッダとして使用する認証時の証明書（セッションキー）を保持する。

【0008】

(3) 前記認証サーバは、予め保持しているアクセスポイントの地理的情報からハンドオーバーし得るアクセスポイントを検索して該当するアクセスポイント部にセッションキーを配布する。

【0009】

(4) 周辺のアクセスポイント部は、前記認証サーバから通知されたセッションキーを保持する。

【0010】

(5) 前記ユーザの無線端末装置がハンドオーバーを行った際に、通信を行うアクセスポイント部が保持しているセッションキーと前記ユーザの無線端末装置のセッションキーとの整合がとれていれば通信を許容する。

【0011】

(6) 初めてパケットの通信を検知したアクセスポイント部は、前記認証サーバにユーザのログインを通知する。

【0012】

(7) 前記認証サーバは、新たにエリア内となったアクセスポイント部へ前記セッションキーを通知し、エリア外となったアクセスポイント部に対しセッション解放を要求する。

【0013】

この通信方式においては、ユーザの無線端末装置がハンドオーバーする可能性のあるアクセスポイント部に対する認証が不要となり、速やかな通信が可能になる。

【0014】

【非特許文献1】

2003年電子情報通信学会総合大会B-6-194「無線LANにおけるハンドオーバーの高速化に関する一考察」

【0015】

【発明が解決しようとする課題】

ところで、無線LANネットワークとしては、例えば、企業内無線LANネットワークと公衆無線LANネットワークとを統合し、これらのネットワーク間を無線端末装置が移動する際に、この無線端末装置の通信サービスをシームレスに継続するようなネットワークが注目されつつある。このような複数の無線LANネットワークを統合したネットワークの形態としては、センター局に前記認証サーバを配置して前記無線端末装置を集中的に管理するネットワークが考えられる

【0016】

ここで、前記センター局で集中管理する形態のネットワークにおいて、各無線 LAN ネットワーク内を無線端末装置が移動して新しいアクセスポイント部にハンドオーバーする場合について考える。この場合、現状の IEEE 802.1X (EAP: Extensible Authentication Protocol) を利用した無線 LAN アクセス認証システムでは、無線端末装置のアクセスポイント部が変わるたびに、前記無線端末装置と前記センター局の認証サーバとの間で認証番号（認証信号）の交換を行う必要がある。このため、この無線 LAN アクセス認証システムにおいては、移動する無線端末装置のアクセス認証及び無線区間の暗号鍵である WEP (Wired Equivalent Privacy) キーの配布に伴って行われる認証手続きにより前記ハンドオーバーに要する時間が増大してパケットロスを招くという問題がある。また、この無線 LAN アクセス認証システムでは、無線端末装置が各アクセスポイント部間を移動するたびに行われる前記無線端末装置と前記センター局との間での認証信号の交換のために、前記センター局と前記各無線 LAN ネットワークとの間の伝送路における認証信号などの制御信号の占有率が増大して、伝送路帯域の有効利用が図れないという問題が発生する。

【0017】

前記従来の通信方式（非特許文献 1 参照）は、このような問題を解消しようとするものである。しかしながら、前述のように、複数の無線 LAN ネットワークを統合し、ユーザ ID 及び無線区間の WEP キー等をセンター局で一元管理しているような大規模なネットワークでは、前記従来の通信方式を適用することが困難となる。

【0018】

すなわち、この複数の無線 LAN ネットワークを統合した大規模なネットワークでは、無線端末装置のアクセス認証に用いるユーザ ID 及び無線区間の WEP キー等が前記センター局で一元管理されている。従って、この大規模なネットワークに前記通信方式を適用した場合には、各無線 LAN ネットワーク間を無線端

末装置がシームレスに移動できるようにするために、無線端末装置が移動するたびに各無線LANネットワークの周辺のアクセスポイント部にWEPキーの配布を行う必要がある。

【0019】

このため、このような大規模なネットワークでは、前記従来の通信方式を取り入れても、前記センター局と前記各無線LANネットワークとの間の伝送路を通して認証信号などの制御信号を頻繁に交換することには変わりはない。また、前記従来の通信方式では、前記センター局の認証サーバが各無線端末装置の位置情報や前記各無線LANネットワークの各アクセスポイント部の地理的情報を管理する必要がある。しかし、このような管理を前記センター局の認証サーバが行うことは、前記認証サーバの負荷をさらに増大させることになる。このようなことから、前述のように複数の無線LANネットワークが統合された大規模のネットワークでは、前記従来の通信方式を適用することが非常に困難である。

【0020】

本発明は、かかる点に鑑みてなされたものであり、複数の無線LANネットワークを統合してセンター局で集中管理するネットワークにおける無線端末装置のアクセス認証の手続きに要する時間を短縮でき、かつ、センター局と各無線LANネットワークとの間の認証信号などの制御信号の数を低減することができる無線LANアクセス認証システムを提供することを目的とする。

【0021】

【課題を解決するための手段】

請求項1記載の無線LANアクセス認証システムは、無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、前記複数の無線LANネットワークの各ゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置とアクセスされた無線端末装置のアクセス認証を行いアクセス認証された無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を配布する認証サーバとを有する前記複数の無線LANネットワークを統合して管理す

るセンター局と、を備え、前記各無線LANネットワークは、各無線LANネットワーク内の無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に該無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理手段と、前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した無線端末装置が前記アクセス管理手段により前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理手段と、を具備する構成を採る。

【0022】

この構成においては、前記無線端末装置が所定の無線LANネットワーク内で移動した場合には、前記アクセス管理手段によりこの無線端末装置の前記認証サーバへのアクセス状況が確認される。そして、この無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合には、前記暗号鍵管理手段により前記暗号鍵が前記無線端末装置及びこの無線端末装置の移動先の新たなアクセスポイント部に配布される。これにより、前記認証サーバに既にアクセスしていることが確認された無線端末装置は、新しいアクセスポイント部に移動する際に、前記センター局の認証サーバとの認証信号の交換を行うことなく、所望の無線LANネットワークへのアクセスが許可される。従って、この構成によれば、無線端末装置の移動に伴うアクセス認証のための認証手続きに要する時間を短縮することができ、前記無線端末装置の新たなアクセスポイント部へのハンドオーバーを容易に行うことができ、前記各無線LANネットワークと前記センター局との間の認証信号などの制御信号の数（認証シグナリング数）を大幅に低減することができ、伝送路の帯域の有効利用を実現することができる。

【0023】

請求項2記載の無線LANアクセス認証システムは、請求項1記載の発明において、前記ゲートウェイ装置は、前記アクセス管理手段及び前記暗号鍵管理手段を有する構成を採る。

【0024】

この構成においては、前記アクセス管理手段及び前記暗号鍵管理手段が、前記各無線LANネットワークの各ゲートウェイ装置に配設されている。従って、この構成によれば、請求項1記載の発明の効果に加えて、前記各無線LANネットワークの構成を簡素化することができる。

【0025】

請求項3記載の無線LANアクセス認証システムは、請求項1又は請求項2記載の発明において、前記アクセス管理手段は、前記各無線端末装置のアクセス時間又は通信パケット量の少なくとも一方のアクセス量を管理し、前記アクセス量が所定量に達した時点で前記無線端末装置に再認証を要求する管理部を有する構成を採る。

【0026】

この構成においては、前記アクセス量が所定量に達した時点で前記管理部より前記無線端末装置に再認証を要求することにより、この無線端末装置が通信する無線区間の暗号鍵を更新することが可能になる。従って、この構成によれば、請求項1又は請求項2記載の発明の効果に加えて、前記暗号鍵の解読による不正無線端末装置の成りすましアクセスを防止することができる。

【0027】

請求項4記載の無線LANアクセス認証システムは、請求項1から請求項3記載のいずれかの発明において、前記無線端末装置はID情報が記録されているSIMカード又はUIMカードを備えており、前記無線端末装置のアクセス認証時の認証用IDとして前記SIMカード又はUIMカードに記録されているID情報を用いる構成を採る。

【0028】

この構成においては、前記無線端末装置のSIMカード又はUIMカードに記録されているID情報が、前記無線端末装置のアクセス認証時の認証用IDとして用いられる。これにより、ユーザが無線端末装置の機種を変更した場合でも、このユーザのアクセス認証時の認証用IDが変更されてしまうことがなくなる。従って、この構成によれば、請求項1乃至請求項3記載のいずれかの発明の効果に加えて、ユーザID及びユーザへの課金を一元管理することができる。

【0029】

請求項5記載の無線LANアクセス認証方法は、無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、前記複数の無線LANネットワークの各ゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置とアクセスされた無線端末装置のアクセス認証を行いアクセス認証された無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を配布する認証サーバとを有する前記複数の無線LANネットワークを統合して管理するセンター局とを備えた無線LANアクセス認証システムにおいて前記無線端末装置のアクセス認証を行う無線LANアクセス認証方法であって、前記各無線LANネットワークが、各無線LANネットワーク内の無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に該無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理ステップと、前記アクセス管理ステップで前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理ステップと、を有するようにした。

【0030】

この方法においては、前記無線端末装置が所定の無線LANネットワーク内で移動した場合には、前記アクセス管理ステップにおいてこの無線端末装置の前記認証サーバへのアクセス状況が確認される。そして、この無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合には、前記暗号鍵管理ステップにおいて前記暗号鍵が前記無線端末装置及びこの無線端末装置の移動先の新たなアクセスポイント部に配布される。これにより、前記認証サーバに既にアクセスしていることが確認された無線端末装置は、新しいアクセスポイント部に移動する際に、前記センター局の認証サーバとの認証信号の交換を行うことなく

、所望の無線LANネットワークへのアクセスが許可される。従って、この構成によれば、無線端末装置の移動に伴うアクセス認証のための認証手続きに要する時間を短縮することができ、前記無線端末装置の新たなアクセスポイント部へのハンドオーバーを容易に行うことができ、前記各無線LANネットワークと前記センター局との間の認証信号などの制御信号の数（認証シグナリング数）を大幅に低減することができ、伝送路の帯域の有効利用を実現することができる。

【0031】

請求項6記載の認証サーバは、無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、前記複数の無線LANネットワークの各ゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置を有する前記複数の無線LANネットワークを統合して管理するセンター局と、を備えた無線LANアクセス認証システムにおいて前記無線端末装置のアクセス認証を行う認証サーバであって、前記認証サーバは、前記センター局に配置され、前記各無線LANネットワークの所定のアクセスポイント部に前記無線端末装置がアクセスするときのアクセス認証を行うアクセス認証手段と、前記各無線LANネットワークの各ゲートウェイ装置に対して前記無線端末装置がアクセスする無線区間の暗号鍵を一括して配布する暗号鍵配布手段と、を有する構成を採る。

【0032】

この構成によれば、前記各無線端末装置のアクセス時のアクセス認証及び前記無線区間の暗号鍵の配布を一括して行うことができ、かつ、前記各無線LANネットワークの各ゲートウェイ装置に前記暗号鍵を配布することができる。

【0033】

請求項7記載のゲートウェイ装置は、無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、前記複数の無線LANネットワークの各ゲートウ

エイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置とアクセスされた無線端末装置のアクセス認証を行いアクセス認証された無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を配布する認証サーバとを有する前記複数の無線LANネットワークを統合して管理するセンター局とを備えた無線LANアクセス認証システムにおける前記各無線LANネットワークのゲートウェイ装置であって、前記ゲートウェイ装置は、前記センター局のセンター局ゲートウェイ装置とのデータ信号及び制御信号の送受信を行う送受信手段と、前記各無線LANネットワーク内の無線端末装置の前記認証サーバへのアクセス状況を管理し前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際にこの無線端末装置の前記認証サーバへのアクセスの有無を確認するアクセス管理手段と、前記アクセス管理手段により前記認証サーバから配布される暗号鍵を管理し他のアクセスポイント部の通信エリアに移動した無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合に前記無線端末装置が通信する無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布する暗号鍵管理手段と、を有する構成を採る。

【0034】

この構成においては、前記ゲートウェイ装置のアクセス管理手段により、前記各無線LANネットワーク内の無線端末装置の前記認証サーバへのアクセス状況が管理される。前記アクセス管理手段は、前記無線端末装置が新たなアクセスポイント部の通信エリアに移動した際に、この無線端末装置の前記認証サーバへのアクセスの有無を確認することができる。また、前記ゲートウェイ装置は、前記無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合に、前記暗号鍵管理手段により前記無線区間の暗号鍵を前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布することができる。従って、この構成によれば、前記無線端末装置の移動に伴う認証手続きに要する時間を短縮することができ、前記無線端末装置の新たなアクセスポイント部へのハンドオーバーを容易に行うことができ、前記各無線LANネットワークと前記センター局との間の認証シグナリング数を大幅に低減することができ、伝送路の帯

域の有効利用を実現することができる。

【0035】

請求項8記載のゲートウェイ装置は、請求項7記載の発明において、前記ゲートウェイ装置のアクセス管理手段は、前記各無線端末装置のアクセス時間又は通信パケット量の少なくとも一方のアクセス量を管理し、前記アクセス量が所定量に達した時点で前記無線端末装置に再認証を要求する管理部を有する構成を採る。

【0036】

この構成においては、前記アクセス量が所定量に達した時点で前記管理部より前記無線端末装置に再認証を要求して、この無線端末装置が通信する無線区間の暗号鍵を更新することが可能となる。従って、この構成によれば、請求項7記載の発明の効果に加えて、前記暗号鍵の解読による不正無線端末装置の成りすましアクセスを防止することができる。

【0037】

請求項9記載の無線端末装置は、無線端末装置が無線区間を通してアクセスする少なくとも2つ以上のアクセスポイント部と前記各アクセスポイント部間のデータ信号及び制御信号の送受信を中継するゲートウェイ装置とを有する複数の無線LANネットワークと、前記複数の無線LANネットワークの各ゲートウェイ装置間のデータ信号及び制御信号の送受信を中継するセンター局ゲートウェイ装置とアクセスされた無線端末装置のアクセス認証を行いアクセス認証された無線端末装置が通信する無線区間の暗号化に用いる暗号鍵を配布する認証サーバとを有する前記複数の無線LANネットワークを統合して管理するセンター局とを備えた無線LANアクセス認証システムにおいて使用される無線端末装置であって、前記無線端末装置は、前記センター局の認証サーバによりアクセス認証される際に用いるID情報が記録されたSIMカード又はUIMカードを有する構成を採る。

【0038】

この構成においては、前記無線端末装置のSIMカード又はUIMカードに記録されているID情報が、前記無線端末装置のアクセス認証時の認証用IDとし

て用いられる。従って、この構成によれば、ユーザが無線端末装置の機種を変更した場合でも、このユーザのアクセス認証時の認証用IDが変更されてしまうことがなくなり、ユーザID及びユーザへの課金を一元管理することができる。

【0039】

【発明の実施の形態】

本発明の骨子は、複数の無線LANネットワークを統合するセンター局の認証サーバへの無線端末装置のアクセス状況を各無線LANネットワークのアクセス管理手段により管理し、新しいアクセスポイント部の通信エリアに移動した無線端末装置が前記認証サーバに既にアクセスしていることが確認された場合に、無線区間の暗号鍵を各無線LANネットワークの暗号鍵管理手段により前記無線端末装置及び前記無線端末装置の移動先の新たなアクセスポイント部に配布することである。

【0040】

以下、本発明の実施の形態について、図面を参照して詳細に説明する。ただし、以下の説明では、無線LANネットワークとして、企業内無線LANネットワークと公衆無線LANネットワークとを統合したネットワークの例を取り上げる。

【0041】

(実施の形態1)

図1は、本発明の実施の形態1に係る無線LANアクセス認証システムを用いたネットワークの構成を示す概略構成図である。図1に示すように、このネットワークは、センター局100、本社内無線LANネットワーク110、支社内無線LANネットワーク120及び公衆無線LANネットワーク130で構成されている。

【0042】

図1において、センター局100は、本社内無線LANネットワーク110、支社内無線LANネットワーク120及び公衆無線LANネットワーク130を集中管理している。また、センター局100には、センター局ゲートウェイ装置101及び認証サーバ102が配置されている。

【0043】

一方、本社内無線LANネットワーク110には、本社内ゲートウェイ装置111、本社内アクセスポイント部112、113、114が配置されている。この本社内無線LANネットワーク110では、ノートパソコン、PDA及び携帯電話などの無線端末装置115、116を用いて通信が行われる。

【0044】

また、支社内無線LANネットワーク120には、支社内ゲートウェイ装置121、支社内アクセスポイント部122、123、124が配置されている。この支社内無線LANネットワーク120では、ノートパソコン、PDA及び携帯電話などの無線端末装置125、126を用いて通信が行われる。

【0045】

また、公衆無線LANネットワーク130には、公衆ゲートウェイ装置131、公衆アクセスポイント部132、133、134が配置されている。この公衆無線LANネットワーク130では、ノートパソコン、PDA及び携帯電話などの無線端末装置135、136を用いて通信が行われる。

【0046】

次いで、この実施の形態1に係る無線LANアクセス認証システムを用いたネットワークの各構成装置の動作について、図2に示すシーケンス図を用いて説明する。

【0047】

図2において、無線端末装置（ここでは、無線端末装置116とする）は、本社内無線LANネットワーク110、支社内無線LANネットワーク120又は公衆無線LANネットワーク130に初めてアクセスするときに、所望のアクセスポイント部（ここでは、本社内アクセスポイント部114とする）にアクセス要求を行う。この無線端末装置116は、無線区間を通して本社内アクセスポイント部114へのアクセスが完了した後、所定の認証手続きを経てアクセス認証される。

【0048】

この認証手続きは、例えば、IEEE802.1Xプロトコルに基づいて、無

線端末装置 116 が、本社内無線 LAN ネットワーク 110 の本社内ゲートウェイ装置 111 及びセンター局 100 のセンター局ゲートウェイ装置 101 を経由して、センター局 100 の認証サーバ 102 にアクセスすることで行われる。

【0049】

この認証手続きでは、図 2 に示すように、本社内アクセスポイント部 114 にアクセス要求を行った無線端末装置 116 に対して、本社内アクセスポイント部 114 から Identity が要求される。無線端末装置 116 は、Identity の要求に対して、ユーザ ID を含む応答信号を本社内アクセスポイント部 114 に送信する。前記応答信号を受信した本社内アクセスポイント部 114 は、無線端末装置 116 の認証信号を本社内ゲートウェイ装置 111 に送信する。

【0050】

なお、ここでは、本社内無線 LAN ネットワーク 110 内の無線端末装置 116 が、本社内アクセスポイント部 114 を通してセンター局 100 の認証サーバ 102 にアクセスする場合について説明したが、他の無線端末装置についても同様に行われる。

【0051】

本実施の形態 1 に係る無線 LAN アクセス認証システムを用いたネットワークの各無線 LAN ネットワーク 110、120、130 に設置されるゲートウェイ装置 111、121、131 は、次のような構成を有している。

【0052】

図 3 は、各ゲートウェイ装置 111、121、131 に共通した構成を有するゲートウェイ装置を示すブロック図である。図 3 に示すように、ゲートウェイ装置 300 は、アクセスポイント部との間でデータの送受信を行うデータ送受信部 301、データ送受信部 301 に対する伝送路を選択するスイッチング部 302、センター局ゲートウェイ装置との間でデータの送受信を行うデータ送受信部 304、データ送受信部 304 に対する伝送路を選択するスイッチング部 303、各無線端末装置のアクセス状況を管理するユーザアクセス管理部 305、及び認証サーバ 102 より配布された暗号鍵（WEP キー）を割り当てられた無線端末装置と対応させて管理する WEP キー管理部 306 を備えている。

【0053】

このゲートウェイ装置300は、前記アクセスポイント部から送られてきたユーザIDを含む応答信号により、アクセス要求のあった無線端末装置のアクセス状況を確認する。ここで、アクセス要求のあった無線端末装置が初期アクセスである場合には、ユーザアクセス管理部305に「アクセスなし」と登録されている。そして、この初期アクセスの場合には、ゲートウェイ装置300が、集中管理を行っているセンター局100のセンター局ゲートウェイ装置101を経由して、認証サーバ102に前記応答信号を転送する。この応答信号を受信した認証サーバ102は、センター局ゲートウェイ装置101、ゲートウェイ装置300、及びアクセスポイント部を経由して、アクセス要求のあった無線端末装置との間で認証シーケンスの交換を行ってこの無線端末装置のアクセス認証を行う。

【0054】

また、認証サーバ102は、前述のようにして無線端末装置のアクセス認証が完了すると、無線端末装置及び各アクセスポイント部に無線区間の暗号鍵であるWEPキーを配布する。このとき、ゲートウェイ装置300は、例えば、アクセス認証が完了した無線端末装置のユーザIDをユーザアクセス管理部305に登録して、アクセス認証が完了した無線端末装置のアクセス状況を管理する。一方、WEPキー管理部306は、配布された暗号鍵(WEPキー)と割り当てられた無線端末装置とを対応させて、アクセス認証が完了した無線端末装置のWEPキーを保存する。WEPキーを配布された無線端末装置とアクセスポイント部とは、このWEPキーを用いて前記無線区間の送受信データを暗号化して通信を行う。

【0055】

次に、ある無線LANネットワークのアクセスポイント部を経由して通信を行っていた無線端末装置が移動して、他の無線LANネットワークのアクセスポイント部を経由して通信するためのアクセス認証を行う場合の動作について説明する。

【0056】

図4は、このようなアクセス認証を行う場合の動作を示すシーケンス図である

。図4において、無線端末装置は、移動先の新たなアクセスポイント部からビーコン（コールサイン及びキャリア）を検知し、新たなアクセスポイント部にアクセス要求を行って、所定の無線区間のアクセス手続きを行う。

【0057】

この無線端末装置は、そのアクセス手続きが完了すると、そのアクセス認証を行うために新しいアクセスポイント部から *Identity* の要求を受ける。この *Identity* の要求により、この無線端末装置は、ユーザIDを含む応答信号を新しいアクセスポイント部に送信する。

【0058】

この応答信号を受信したアクセスポイント部は、無線端末装置からの応答信号をゲートウェイ装置300に送信する。ゲートウェイ装置300は、このアクセスポイント部から送られてきたユーザIDを含む応答信号に基づいて、ユーザアクセス管理部305によりアクセス要求のあったユーザの無線端末装置のアクセス状況を確認する。

【0059】

ここで、アクセス要求のあったユーザの無線端末装置が、前述した初期アクセスにより既に登録されている場合には、ゲートウェイ装置300が、WEPキー管理部306でアクセス要求をしてきた無線端末装置に割り当てられているWEPキーを検索し、予め登録されているWEPキーを移動先の新しいアクセスポイント部及びアクセス要求のあった無線端末装置に再配布する。このようにしてWEPキーを配布された無線端末装置とアクセスポイント部とは、再配布されたWEPキーを用いて所定の無線区間の送受信データを暗号化して通信を行う。

【0060】

ここで、ユーザアクセス管理部305及びWEPキー管理部306は、前記各無線端末装置のアクセス状況及び割り当てられたWEPキーの管理を行うとともに、図示しないタイムアウト機能により、一定時間アクセス要求のない無線端末装置に対する登録を抹消して、電源のOFF及び他のドメインへの移動などにも対応する。

【0061】

また、ここでは、ゲートウェイ装置 300 に、ユーザのアクセス状況及び WEP キーを管理するユーザアクセス管理部 305 及び WEP キー管理部 306 を配設する構成としたが、これらのユーザアクセス管理部 305 及び WEP キー管理部 306 は、ゲートウェイ装置 300 から分離して、各無線 LAN ネットワークに独立して配置した構成とすることも可能である。

【0062】

このように、本実施の形態 1 に係る無線 LAN アクセス認証システムにおいては、無線端末装置が移動して新しいアクセスポイント部にアクセスする際のアクセス認証及び WEP キーの配布を、各無線 LAN ネットワークに配置したゲートウェイ装置 111、121、131で行うことができるので、無線端末装置の移動に伴うアクセス認証手続きに要する時間を短縮することができる。これにより、本実施の形態 1 に係る無線 LAN アクセス認証システムにおいては、無線端末装置の移動時のハンドオーバーにかかる時間の短縮化、及び各無線 LAN ネットワークとセンター局 100 との間の認証シグナリング数を大幅に低減して、伝送路の帯域の有効利用を実現することができる。

【0063】

(実施の形態 2)

次に、本発明の実施の形態 2 について、図面を参照して詳細に説明する。

本発明の実施の形態 2 に係る無線 LAN アクセス認証システムは、本発明の実施の形態 1 に係る無線 LAN アクセス認証システムの機能に加えて、無線端末装置のアクセス時間及び通信パケット量をカウントする機能を有している。そして、この実施の形態 2 に係る無線 LAN アクセス認証システムでは、無線端末装置のアクセス時間もしくは通信パケット量が所定量に達した時点で、前記無線端末装置にセンター局 100 の認証サーバ 102 との再認証及び新しい暗号鍵の配布が要求される。

【0064】

図 5 は、本実施の形態 2 に係る無線 LAN アクセス認証システムで使用されるゲートウェイ装置の構成を示す。なお、この実施の形態 2 に係る無線 LAN アクセス認証システムで使用されるゲートウェイ装置において、図 3 に示したゲート

ウエイ装置 300 と同一の機能を有する構成要素には同一符号を付して、その詳細な説明を省略する。

【0065】

図5に示すように、本実施の形態2に係る無線LANアクセス認証システムで使用されるゲートウェイ装置 500 は、各無線端末装置のアクセス状況を管理するユーザアクセス管理部 501 が、アクセス時間管理部 502 及び通信パケット量管理部 503 を備えている。アクセス時間管理部 502 は、各無線端末装置のアクセス時間をカウントするように構成されている。また、通信パケット量管理部 503 は、各無線端末装置の通信パケット量をカウントするように構成されている。

【0066】

次に、本実施の形態2に係る無線LANアクセス認証システムにおける無線端末装置の再認証及び暗号鍵の再配布までの動作について説明する。図6は、この実施の形態2に係る無線LANアクセス認証システムにおける無線端末装置の再認証及び暗号鍵の再配布までの動作を示すシーケンス図である。

【0067】

図6において、アクセス要求のあった無線端末装置と認証サーバ 102 とのアクセス認証が完了すると、無線端末装置は所望のネットワークとの通信を開始する。また、これと同時に、ゲートウェイ装置 500 のアクセス時間管理部 502 及び通信パケット量管理部 503 が、無線端末装置のアクセス時間及びパケット量のカウントを開始する。

【0068】

ここで、あるアクセスポイント部を経由して通信している無線端末装置が移動し、新しいアクセスポイント部を経由して通信を行おうとする場合には、ゲートウェイ装置 500 の WEP キー管理部 306 に管理されている暗号鍵 (WEP キー) が、この無線端末装置及び移動先の新しいアクセスポイント部に再配布される。これにより、この無線端末装置は、そのアクセス認証時に配布された暗号鍵と同じ暗号鍵を用いて通信が行われる。

【0069】

その後、ゲートウェイ装置500のアクセス時間管理部502及び通信パケット量管理部503によりカウントされたアクセス時間もしくは通信パッケージ量が所定量に達すると、ゲートウェイ装置500は、アクセスしている無線端末装置に対してセンター局100の認証サーバ102との間で再認証と暗号鍵の再配布手続きを行うように要求信号を通知する。

【0070】

このとき、ゲートウェイ装置500のユーザアクセス管理部501により管理されているユーザのアクセス状況の登録内容は、再認証が必要な状態であるという内容に変更される。また、無線LANアクセス認証システムの通信モードは、無線端末装置から送られてくる認証信号をセンター局100の認証サーバ102に転送するモードに切り換えられる。

【0071】

これにより、前記再認証及び暗号鍵の再配布の要求信号を受け取った無線端末装置が、所定のアクセスポイント部に認証要求信号を送信することにより、図6に示す一連の認証シーケンスが開始される。そして、IEEE802.1Xプロトコルに基づく所定の認証手続きが完了すると、新しい暗号鍵(WEPキー)が認証サーバ102より配付され、移動した無線端末装置と移動先の新しいアクセスポイント部とが、この新しい暗号鍵を用いて送信データの暗号化を行って通信を行う。また、これと同時に、ゲートウェイ装置500は、WEPキー管理部306により新しい暗号鍵を保存し、アクセス時間管理部502及び通信パケット量管理部503により再び無線端末装置のアクセス時間及びパケット量のカウンタを開始する。

【0072】

このように、本実施の形態2に係る無線LANアクセス認証システムにおいては、ゲートウェイ装置500のアクセス時間管理部502及び通信パケット量管理部503により、無線端末装置のアクセス時間及びパケット量が管理されている。

【0073】

そして、アクセスしている無線端末装置のアクセス時間及び通信パケット量が

所定量に達した時点で、この無線端末装置に、センター局100の認証サーバ102との間で、アクセス認証の再認証と暗号鍵の再配布との手続きを行うように要求される。

【0074】

従って、本実施の形態2に係る無線LANアクセス認証システムによれば、アクセスしている無線端末装置のアクセス時間及び通信パケット量が所定量に達する毎に、無線端末装置とアクセスポイント部との間で使用される暗号鍵（WEPキー）が更新され、WEPキーの解読などによる成りすましアクセスを防止することができる。

【0075】

（実施の形態3）

次に、本発明の実施の形態3について、図面を参照して詳細に説明する。

本発明の実施の形態3に係る無線LANアクセス認証システムは、前記各無線端末装置がSIM（Subscriber Identity Module）カードを搭載しており、このSIMカード内から前述のアクセス認証に用いるユーザIDを抽出してアクセス認証の手続きを行うものである。

【0076】

図7は、本実施の形態3に係る無線LANアクセス認証システムで使用する無線端末装置の構成を示すブロック図である。図7に示すように、この無線端末装置700は、無線LAN I/F 701（無線LAN用のアクセスインターフェース）、SIMカード702、EAPクライアント703、及びWEPクライアント704を備えている。

【0077】

この無線端末装置700では、IEEE802.1x（EAP: Extensible Authentication Protocol）機能を有するEAPクライアント703が、センター局100の認証サーバ102との間で、認証信号の交換を行う。そして、SIMカード702内に記録されているユーザIDを使用して、IEEE802.1xのシーケンスが遂行される。

【0078】

なお、SIMカード702内に記録されているユーザIDは、センター局100の認証サーバ102にも登録されている。また、無線端末装置は、WEPクライアント704により、アクセス認証後、認証サーバ102から付与された暗号鍵を用いて暗号化及び複合化を行う。

【0079】

図8は、本実施の形態3に係る無線LANアクセス認証システムで使用する他の無線端末装置の構成を示すブロック図である。図8に示すように、この無線端末装置800は、図7に示した無線端末装置700の構成に加えて、セルラー無線I/F801及びセルラー認証クライアント802を備えている。すなわち、この無線端末装置800は、無線LAN用のアクセスインターフェースである無線LAN I/F701に加えて、セルラー無線用のアクセスインターフェースであるセルラー無線I/F801を有している。

【0080】

この無線端末装置800では、図8に示すように、SIMカード702に記録されたユーザIDがEAPクライアント703に与えられて、無線LANネットワーク側のアクセス認証に使用される。

【0081】

また、この無線端末装置800では、SIMカード702に記録されたユーザIDがセルラー無線ネットワーク側の認証を行うセルラー認証クライアント802にも与えられ、セルラー無線ネットワーク側のアクセス認証にも使用される。

【0082】

なお、ここでは、無線端末装置に搭載したSIMカード702のユーザIDをアクセス認証に使用する例について説明したが、アクセス認証に使用するユーザ情報としては、例えば、第3世代携帯電話端末に搭載されているUIM (User Identity Module) カードに記録されているユーザ情報を使用しても同様な認証手続きを行うことができる。

【0083】

従って、本実施の形態3に係る無線LANアクセス認証システムによれば、ユーザが無線端末装置の機種を変更した場合でも、このユーザのアクセス認証時の

認証用IDが変更されてしまうことがなくなり、ユーザID及びユーザへの課金を一元管理することができるほか、セルラー無線ネットワークと無線LANネットワークとの両ネットワークのアクセス認証及び課金に対しても一元化を行うことができる。

【0084】

【発明の効果】

以上説明したように、本発明によれば、無線端末装置の移動に伴うアクセス認証のための認証手続きに要する時間を短縮することができ、前記無線端末装置の新たなアクセスポイント部へのハンドオーバーを容易に行うことができ、前記各無線LANネットワークと前記センター局との間の認証信号などの制御信号の数（認証シグナリング数）を大幅に低減することができ、かつ、伝送路の帯域の有効利用を実現することができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態1に係る無線LANアクセス認証システムの構成を示す概略構成図

【図2】

本発明の実施の形態1に係る無線LANアクセス認証システムにおける認証シーケンスを示す図

【図3】

本発明の実施の形態1に係る無線LANアクセス認証システムで使用する各無線LANネットワークのゲートウェイ装置の構成を示すブロック図

【図4】

本発明の実施の形態1に係る無線LANアクセス認証システムにおいて無線端末装置が移動するときのアクセス認証の動作を示すシーケンス図

【図5】

本発明の実施の形態2に係る無線LANアクセス認証システムで使用する各無線LANネットワークのゲートウェイ装置の構成を示すブロック図

【図6】

本発明の実施の形態 2 に係る無線 LAN アクセス認証システムにおいて無線端末装置が移動するときのアクセス認証の動作を示すシーケンス図

【図 7】

本発明の実施の形態 3 に係る無線 LAN アクセス認証システムに使用する無線端末装置の構成を示すブロック図

【図 8】

本発明の実施の形態 3 に係る無線 LAN アクセス認証システムに使用する無線端末装置の他の構成を示すブロック図

【符号の説明】

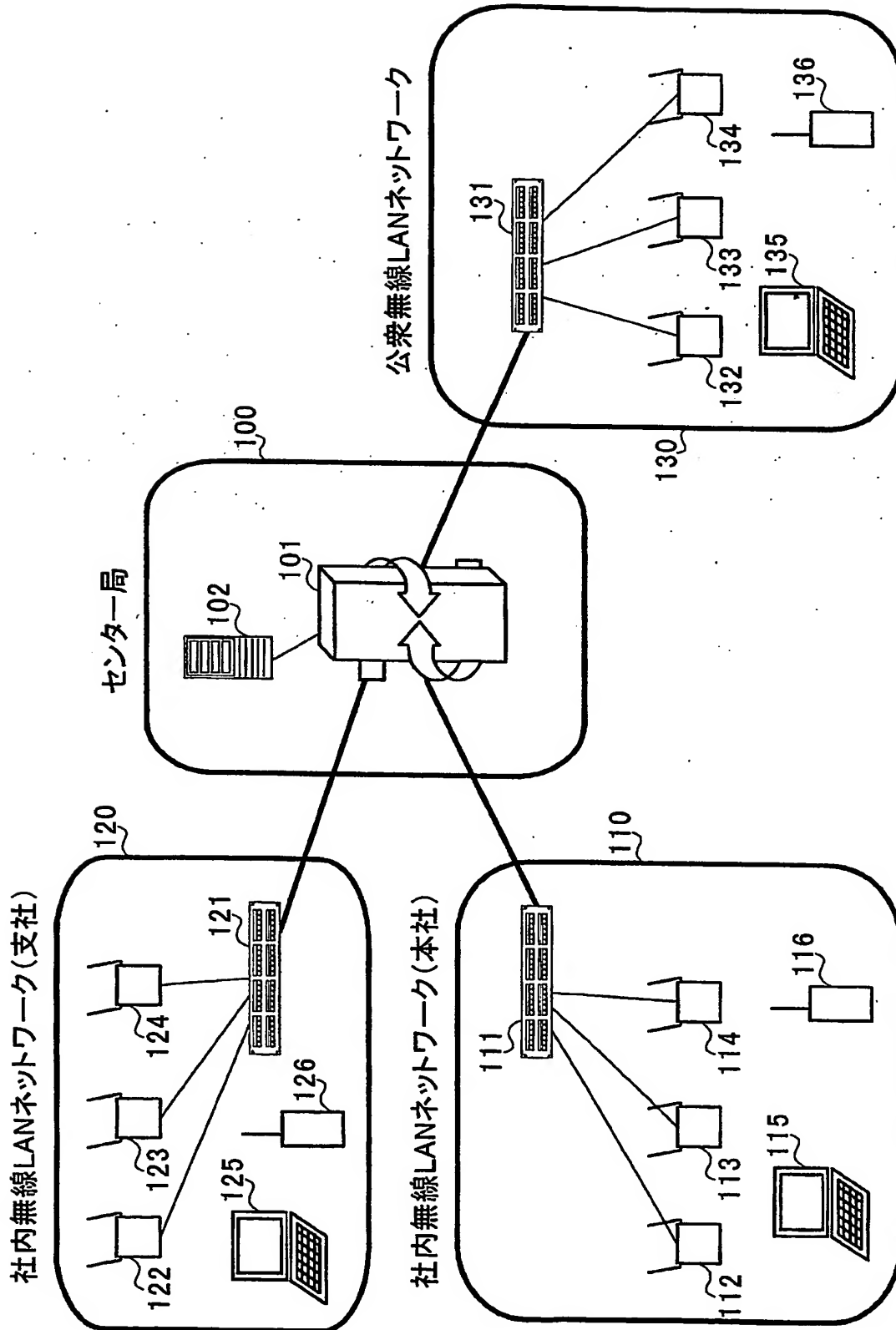
- 100 センター局
- 101 センター局ゲートウェイ装置
- 102 認証サーバ
- 110 本社内無線 LAN ネットワーク
- 111 本社内ゲートウェイ装置
- 112、113、114 本社内アクセスポイント部
- 115、116、125、126、135、136 無線端末装置
- 120 支社内無線 LAN ネットワーク
- 121 支社内ゲートウェイ装置
- 122、123、124 支社内アクセスポイント部
- 130 公衆無線 LAN ネットワーク
- 131 公衆ゲートウェイ装置
- 132、133、134 公衆アクセスポイント部
- 300、500 ゲートウェイ装置
- 301、304 データ送受信部
- 302、303 スイッチング部
- 305 ユーザアクセス管理部
- 306 WEP キー管理部
- 501 ユーザアクセス管理部
- 502 アクセス時間管理部

503 通信パケット量管理部
700、800 移動端末装置
701 無線LAN I/F
702 SIMカード
703 EAPクライアント
704 WEPクライアント
801 セルラー無線 I/F
802 セルラー認証クライアント

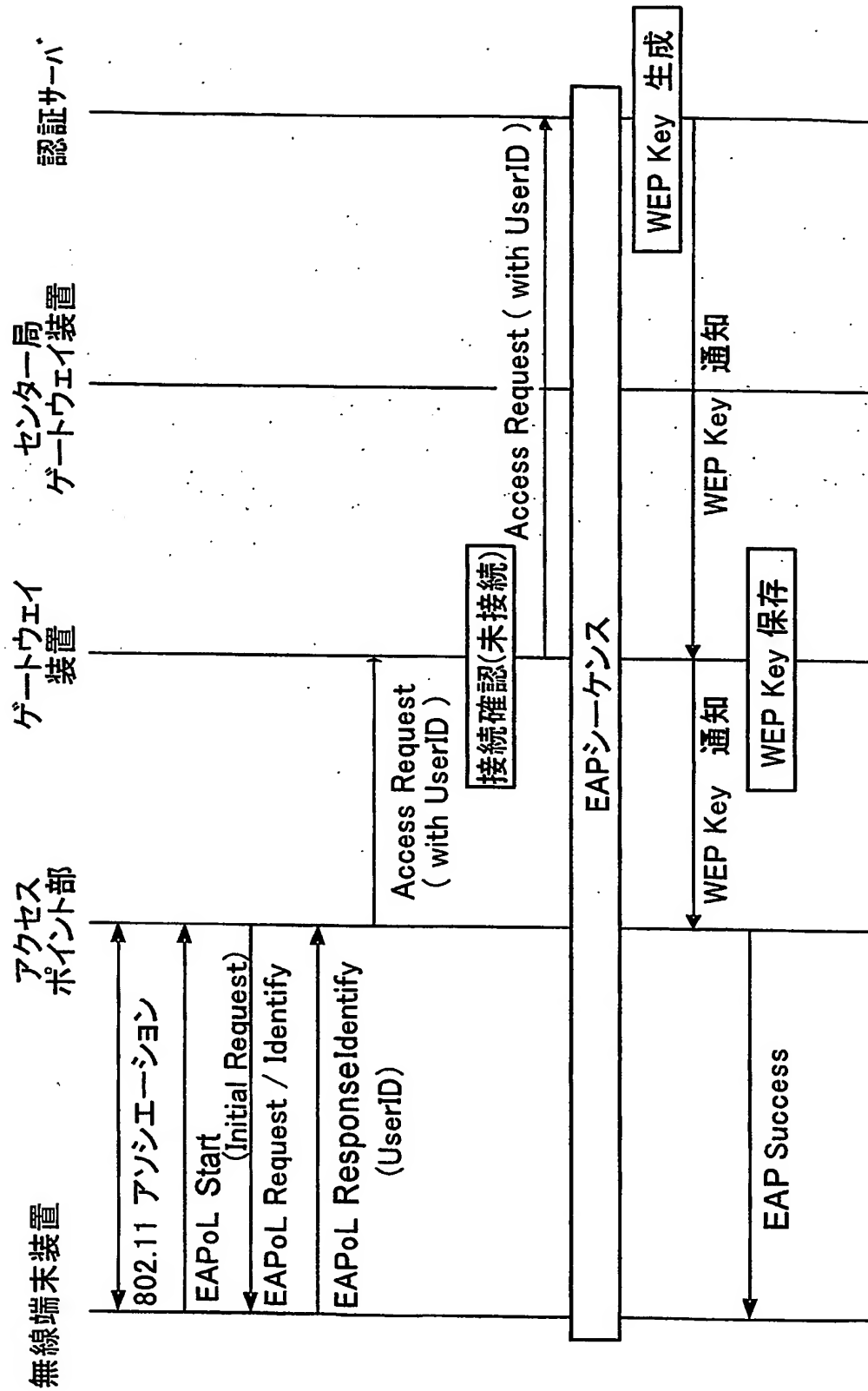
【書類名】

図面

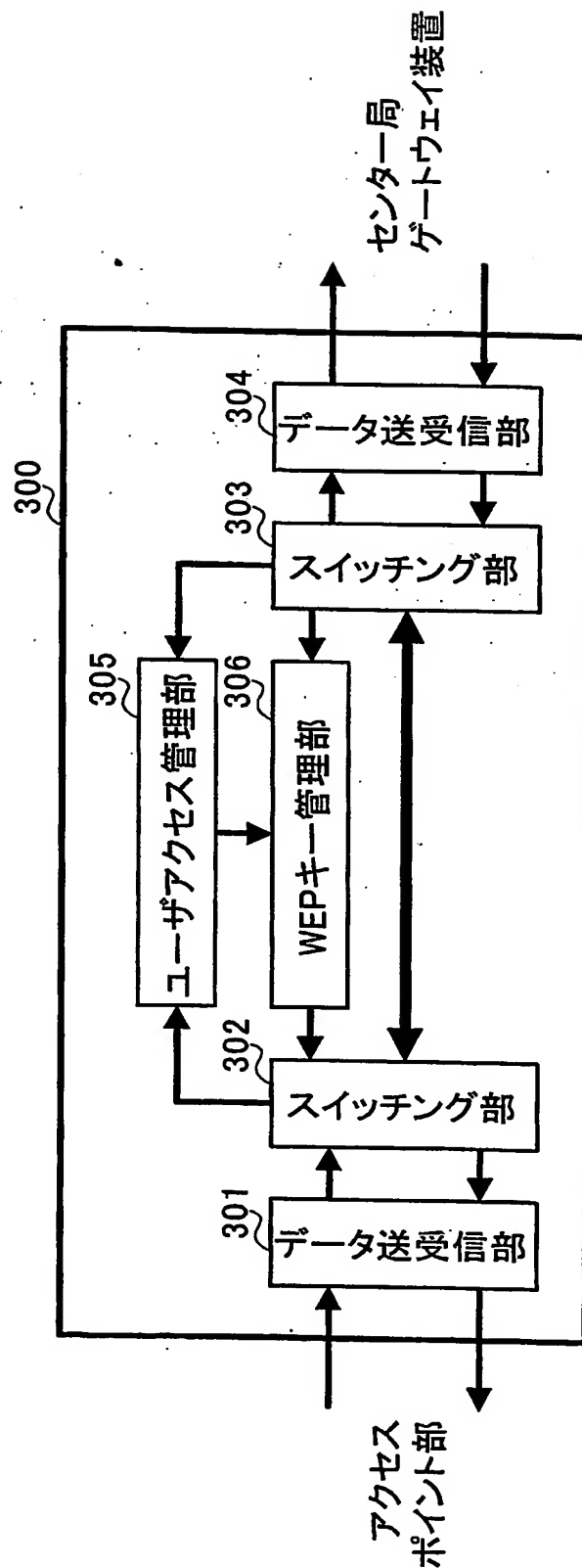
【図 1】



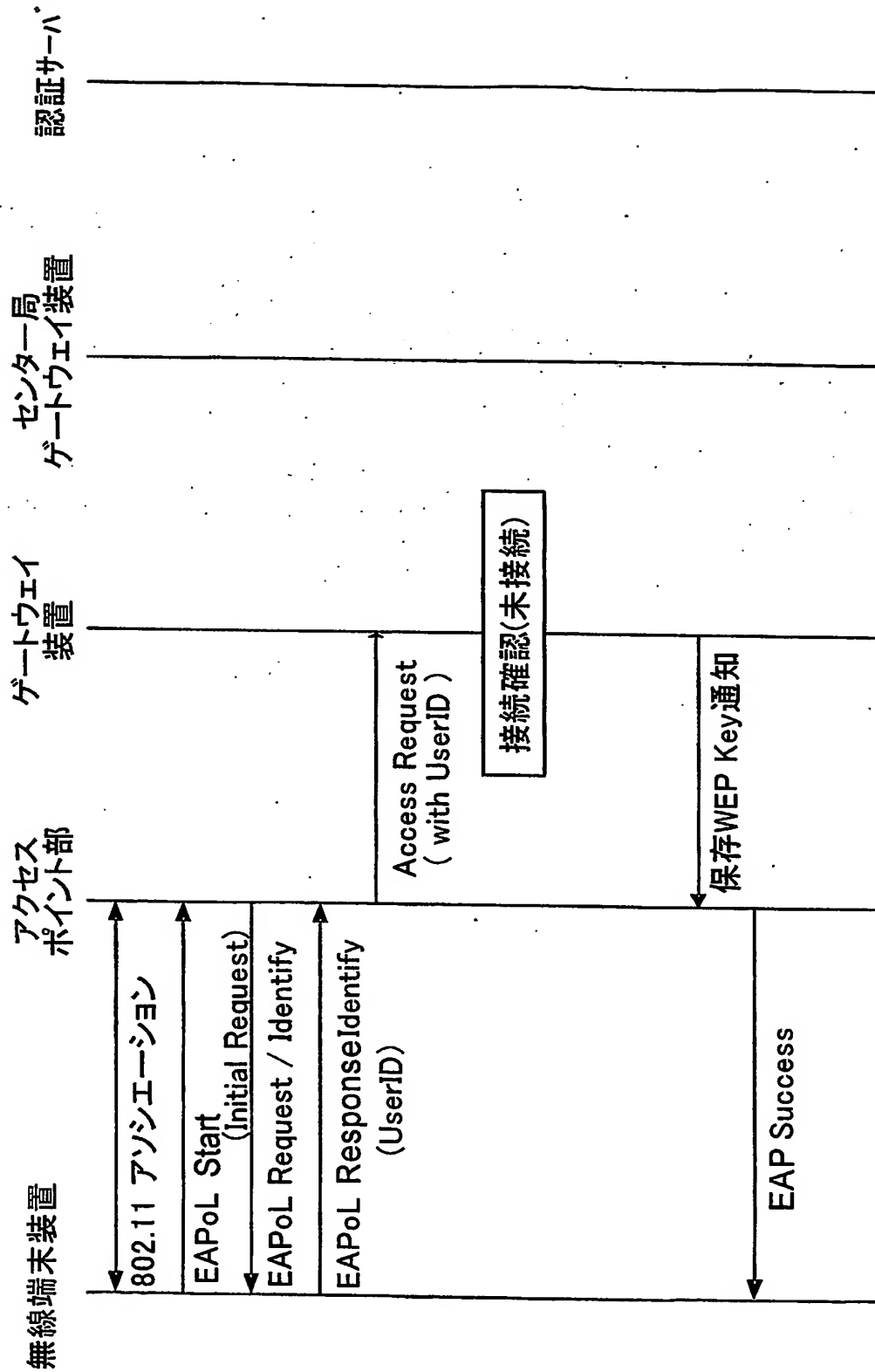
【図 2】



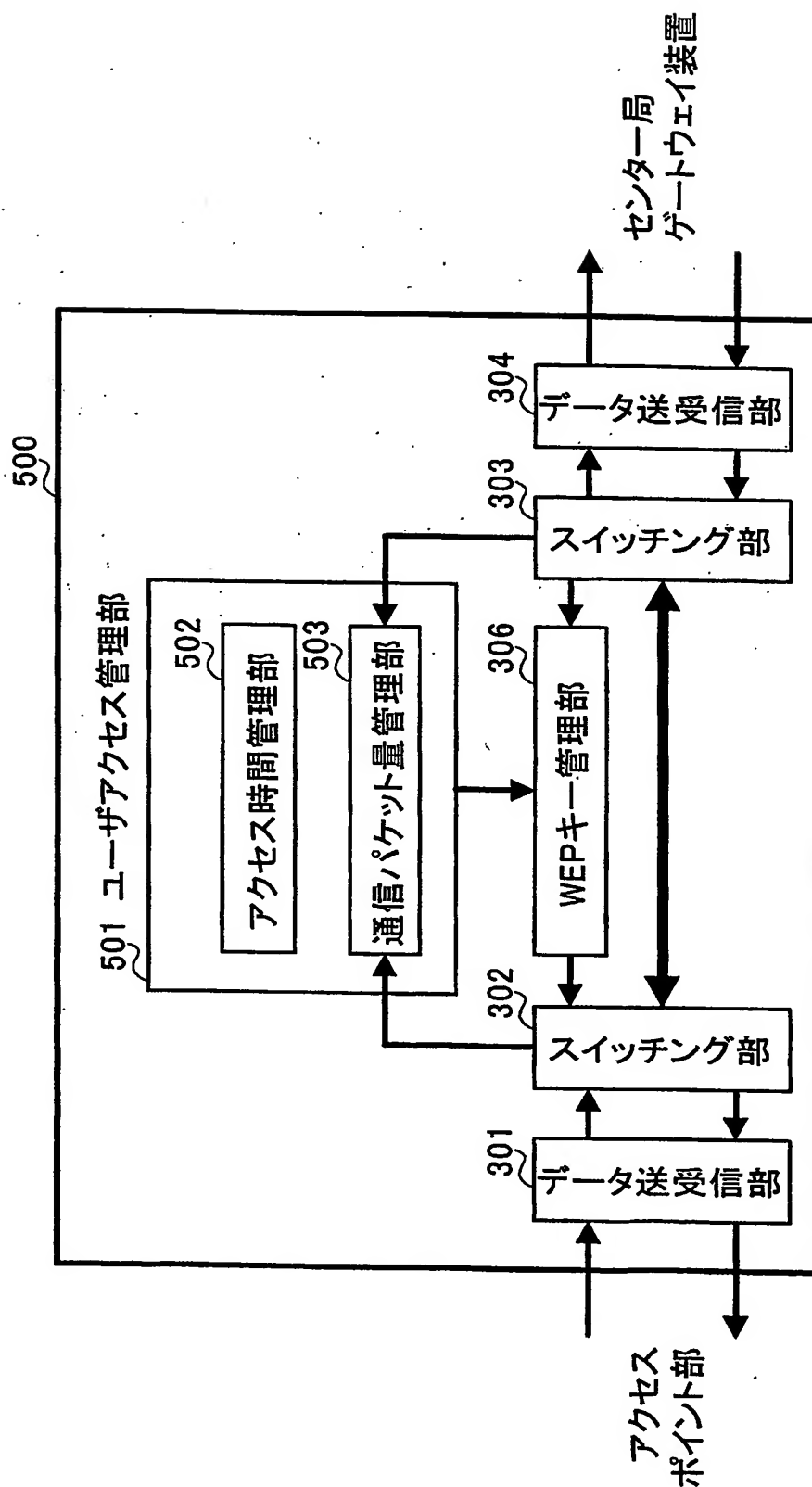
【図 3】



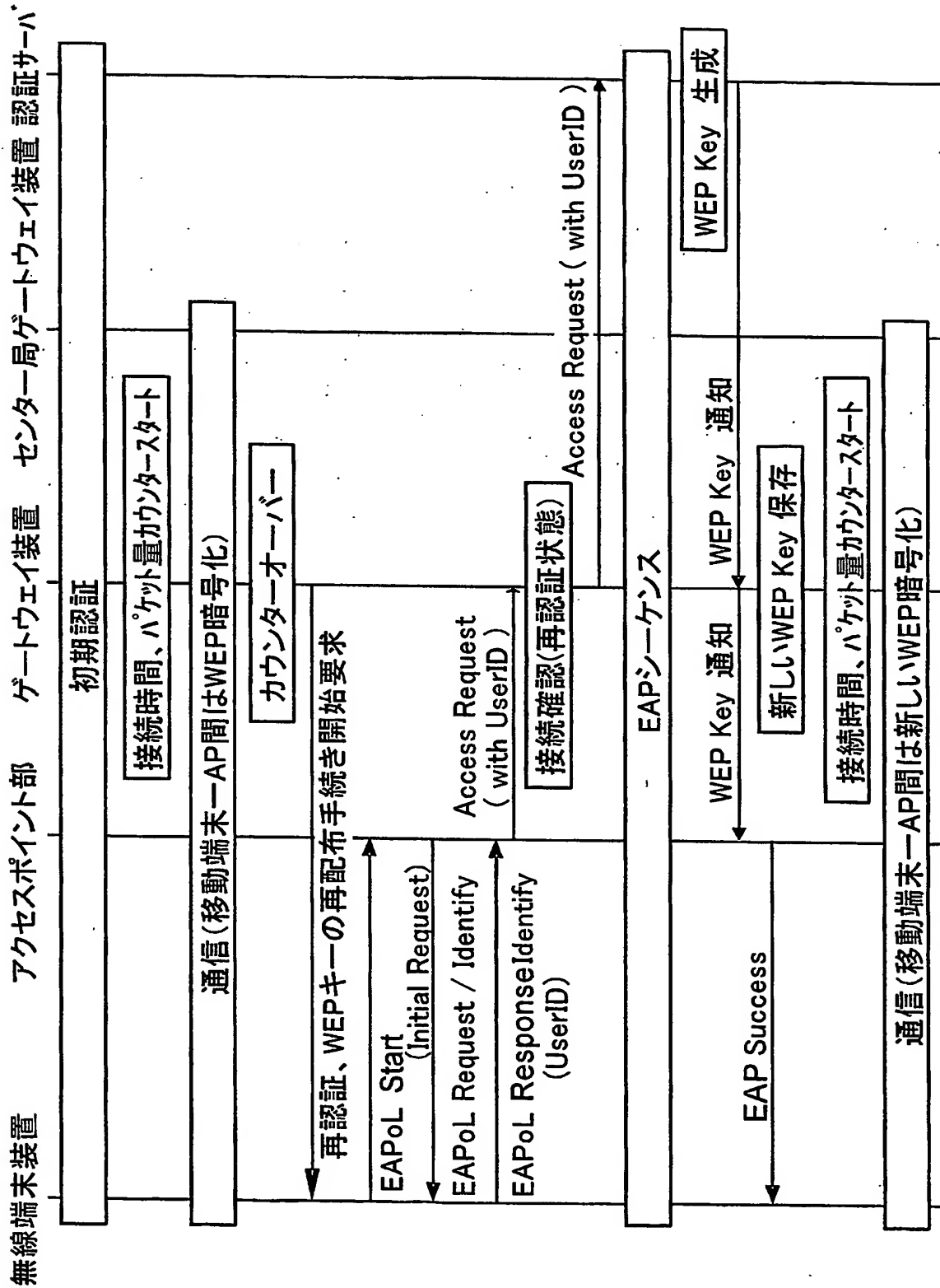
【図 4】



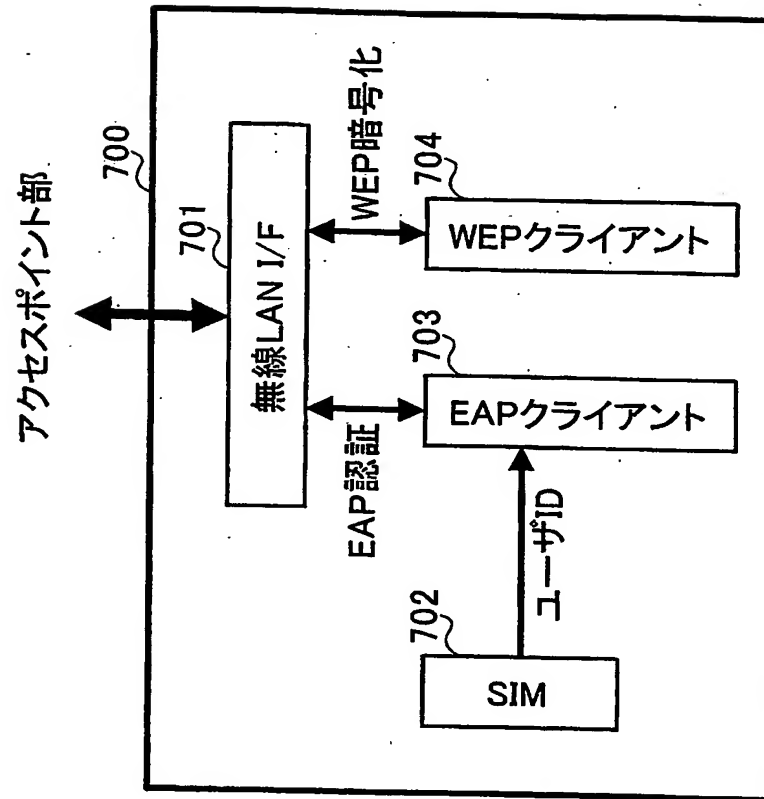
【図 5】



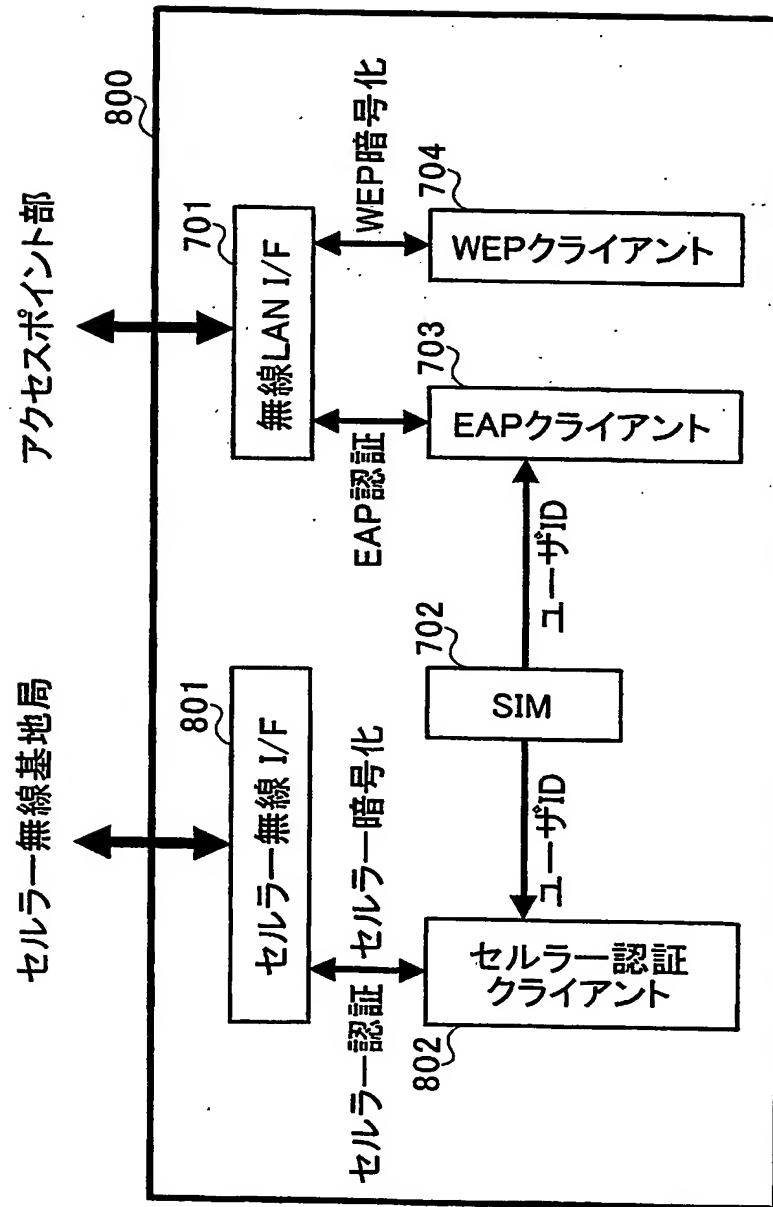
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 複数の無線LANネットワークを統合してセンター局で集中管理するネットワークにおける無線端末装置のアクセス認証の手續きに要する時間を短縮でき、かつ、センター局と各無線LANネットワークとの間の認証信号などの制御信号の数を低減すること。

【解決手段】 アクセス要求のあったユーザの無線端末装置が、初期アクセスにより既に登録されている場合には、ゲートウェイ装置300が、WEPキー管理部306でアクセス要求をしてきた無線端末装置に割り当てられているWEPキーを検索し、予め登録されているWEPキーを移動先の新しいアクセスポイント部及びアクセス要求のあった無線端末装置に再配布する。WEPキーを配布された無線端末装置とアクセスポイント部とは、再配布されたWEPキーを用いて所定の無線区間の送受信データを暗号化して通信を行う。

【選択図】 図1

特願2003-137830

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住 所

大阪府門真市大字門真1006番地

氏 名

松下電器産業株式会社